DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Accountability		Process allowing auditing of information system activities to be traced to a source that may then be held responsible.
Accreditation	DODD 5000.59	The official certification that a model or simulation is acceptable for use for a specific purpose.
Acquisition Category (ACAT)	AFPD 63-1, Jul 03	Categories created to decentralize decision-making for acquisition programs. The categories determine the decision authority, level of review, and applicable procedures and statutorily imposed requirements.
Acquisition Center of Excellence (ACE)	AFPD 63-1, Jul 03	Established by the Air Force to serve as the transformation agent for delivering capabilities to the warfighter by instilling radical changes to the acquisition process and removing obstacles that inhibit that transformation. All actions of the ACE will be directed towards accelerating the delivery of required, affordable, capable products that enable the transformation and increase credibility in program promises.
Acquisition Facilities	DoD 5200.1-M, Mar 94	DoD facilities primarily involved in activities related to research, development of systems, testing, or evaluation of test results.
Acquisition Program	AFPD 63-1, Jul 03	A directed, funded effort designed to provide a new, improved, or continuing materiel, weapon, or information system capability in response to a validated operational or business need that supports operational requirements. Acquisition programs are designated by the Acquisition Executive to fall within categories which are established to facilitate decentralized decision-making, execution, and compliance with statutory requirements. Technology projects, service contracts or supply contracts that have not been designated as ACATs are not acquisition programs.
Acquisition Program	DODD 5000.1 DODD 5200.39, Sep 97	A directed, funded effort that is designed to provide a new, improved, or continuing weapons system or automated information system capability in response to a validated operational need. Acquisition programs are divided into categories, which are established to facilitate decentralized decision-making and execution and compliance with statutory requirements.
Acquisition Program	DODD 5205.2	A directed and funded effort that is designed to provide a new, improved, or continuing weapons system or automated information system capability in response to a validated operational need.
Acquisition Program Baseline (APB)	CJCSI 3170.01D, Mar 04	Each program's APB is developed and updated by the program manager and will govern the activity by prescribing the cost, schedule and performance constraints in the phase succeeding the milestone for which it was developed.
Acquisition Systems Protection (ASP)	DoD 5200.1-M, Mar 94	The safeguarding of defense systems anywhere in the acquisition process as defined in DoD Directive 5000.1, the defense technologies being developed that could lead to weapon or defense systems, and defense research data. ASP integrates all security disciplines, counterintelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver to our forces uncompromised combat effectiveness over the life expectancy of the system.
Administrative Instruction	DoD 5025.1-M	A DoD issuance that implements policies and tells the Washington Headquarters Services (WHS) Components and National Capital Region (NCR) agencies how to carry out a policy, operate a program or activity, and assign responsibilities as directed by the Director, WHS.
Advanced Concept Technology Demonstration (ACTD)	CJCSI 3170.01D, Mar 04	A demonstration of the military utility of a significant new technology and an assessment to clearly establish operational utility and system integrity.
Adversary	DoD 5200.1-M, Mar 94	An individual, group, organization, or government that must be denied essential information.
Air Force Acquisition Executive (AFAE)	AFPD 63-1, Jul 03	The Assistant Secretary of the Air Force (Acquisition), ASAF(A), is designated by the Secretary of the Air Force Order 101.1, Authority and Responsibilities of the Assistant Secretary of the Air Force (Acquisition), June 5, 1999, as the AFAE and is accountable to the Secretary of the Air Force (SECAF) for all domestic and international Air Force acquisition functions, including Foreign Military Sales programs.
Analysis of Alternatives (AoA)	CJCSI 3170.01D, Mar 04	The evaluation of the operational effectiveness, operational suitability and estimated costs of alternative systems to meet a mission capability. The analysis assesses the advantages and disadvantages of alternatives being considered to satisfy capabilities, including the sensitivity of each alternative to possible changes in key assumptions or variables.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Anomaly detection system		Detector configured to identify behavior that deviates from normal system usage.
Anti-Tamper	AFPD 63-17	The systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems.
Anti-Tamper Techniques	AT Implementation Guidelines, USD, May 00	Systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems
Application	DODD 8500.1	Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.
Application Specific Integrated Circuit (ASIC)		An integrated circuit designed to perform a particular function by defining the interconnection of a set of basic circuit building blocks drawn from a library provided by the circuit manufacturer.
Architecture	CJCSI 3170.01D, Mar 04	The structure of components, their relationships and the principles and guidelines governing their design and evolution over time. attribute - A testable or measurable characteristic that describes an aspect of a system or capability.
Architectures	DODD 4630.5	The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.
Authentication	DODD 8500.1	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (i)).
Authentication		Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Authorized User	DODD 8500.1	Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.
Automated Information System (AIS) Application	AFPD 63-1, Jul 03	An acquisition program that acquires information Technology (IT), except IT that: 1) involves equipment that is an integral part of a weapon or weapons system; or 2) is a tactical communication system.
Automated Information System (AIS) Application	DODD 8500.1	For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in reference (k). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS)). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in reference (j); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).
Availability	DODD 8500.1	Timely, reliable access to data and information services for authorized users (reference (i)).
Balanced Risk	AFPD 63-1, Jul 03	A rational consideration of the likely magnitude of various inherent risks, such as technology, time, cost, etc, resulting in a plan of action that accepts program risk in one or more areas.
Biometrics		Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.
BREADBOARD	INTERIM DEFENSE ACQUISITION GUIDEBOOK	Integrated components that provide a representation of a system/subsystem and which can be used to determine concept feasibility and to develop technical data. Typically configured for laboratory use to demonstrate the technical principles of immediate interest. May resemble final system/subsystem in function only.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Capability	CJCSI 3170.01D, Mar 04	The ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a DOTMLPF change recommendation. In the case of material proposals, the definition will progressively evolve to DOTMLPF performance attributes identified in the CDD and the CPD.
Capability Development Document (CDD)	CJCSI 3170.01D, Mar 04	A document that captures the information necessary to develop a proposed program(s), normally using an.CJCSI 3170.01D evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability capability gaps - Those synergistic resources that are unavailable but potentially attainable to the operational user for effective task execution. These resources may come from the entire range of DOTMLPF solutions.
Certification	CJCSI 3170.01D, Mar 04	A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process.
Classified Military Equipment		Military equipment that is itself classified; contains classified information that may be derived from or revealed by its operation or testing; or will require the disclosure of classified information for operation, employment, maintenance, or training.
Classified Military Information		Information originated by or for the Department of Defense or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL, as described in E.O. 12356 (reference (q)). Classified military information may be in oral, visual, or material form and has been subdivided further into the following eight categories:
Classified Military Information Category 1 - Organization, Training, and Employment of Military Forces		Information of a general nature pertaining to tactics, techniques, tactical doctrine, and intelligence and counterintelligence doctrine and techniques. Excluded is information necessary for the operation, training, and maintenance on specific equipment covered under Categories 2 and 3, below.
Classified Military Information Category 2 - Military Materiel and Munitions		Information on specific items of equipment already in production, or in service, and the information necessary for the operation, maintenance, and training. Items on the U.S. Munitions List fall within this category. This category does not pertain to equipment that is in research and development.
Classified Military Information Category 3 - Applied Research and Development Information and Materiel		Information related to fundamental theories, design, and experimental investigation into possible military applications; it includes engineering data, operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when the equipment has completed suitability testing and has been adopted for use or production.
Classified Military Information Category 4 - Production Information		Information related to designs, specifications, manufacturing techniques, and such related information necessary to manufacture materiel and munitions.
Classified Military Information Category 5 - Combined Military Operations, Planning, and Readiness		Information necessary to plan, ensure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. It does not include strategic plans and guidance or North American defense information.
Classified Military Information Category 6 - U.S. Order of Battle		Information pertaining to U.S. forces in a specific area. In general, disclosures of this information are limited to those countries in which U.S. forces are stationed or are in adjacent geographical areas.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Classified Military Information Category 7 - North American Defense		Information related to plans, operations, programs, and projects, to include data and equipment, directly related to North American defense.
Classified Military Information Category 8 - Military Intelligence		Information of a military character pertaining to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the Director of Central Intelligence (DCI).
Commander's Intent	AFPD 63-1, Jul 03	A device designed to help subordinates understand the larger context of their actions. The purpose of providing intent is to allow subordinates to exercise judgment and initiative—to depart from the original plan when the unforeseen occurs—in a way that is consistent with higher commanders' aims.
Common-use M&S	DODD 5000.59	M&S applications, services, or materials provided by a DoD Component to two or more DoD Components.
Community Risk	DODD 8500.1	Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.
Component Acquisition Executive (CAE)	AFPD 63-1, Jul 03	The official responsible for systems acquisitions in the Air Force. Sometimes the CAE is also referred to as the Service Acquisition Executive (SAE). The Assistant Secretary of the Air Force (Acquisition) is the CAE for non-space related programs. The Undersecretary of the Air Force is the CAE for space related programs.
Component Intelligence (Counterintelligence) Analysis Centers	DoD 5200.1-M, Mar 94	Within this Manual, the organizations of the DoD Components that produce the Multi-Discipline Counterintelligence (MDCI) Threat Assessments for use in program protection planning. In some DoD Components, these organizations are labeled as intelligence organizations, while in others they are part of counterintelligence organizations.
Compromise	DODD 5200.1	A communication or physical transfer of classified information to an unauthorized recipient.
Compromise	DoD 5200.1-M, Mar 94	The known or suspected exposure of EPITS or classified information or material to persons who are not authorized access.
Computer Network	DODD 8500.1	The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan or wide area and backbone networks.
Computing Environment	DODD 8500.1	Workstation or server (host) and its operating system, peripherals, and applications (reference (i)).
Confidentiality	DODD 8500.1	Assurance that information is not disclosed to unauthorized entities or processes (reference (i)).
Connection Approval	DODD 8500.1	Formal authorization to interconnect information systems.
Contractor Owned/Contract Operated (COCO)	AFPD 63-17, Nov 01	An industrial facility owned and operated by a contractor.
Controlled Unclassified Information	DODD 8500.1	Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes U.S. information that is determined to be exempt from public disclosure in accordance with DoD Directives 5230.25 and 5400.7 (references (r) and (s)) or that is subject to export controls in accordance with the ITAR (reference (f)) or the EAR (reference (t)).
Cooperative Development	DODD 5000.59	A project in which two or more DoD Components share in domain research, technical studies, or technology development but that may result in dissimilar M&S applications.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Cooperative Research and Development Agreement (CRADA)	DODI 5535.8, May 99	An agreement between one or more Federal laboratories and/or technical activities and one or more non-Federal parties. Under a CRADA, the Government laboratories and/or technical activities shall provide personnel, services, facilities, equipment or other resources with or without reimbursement (but not funds to the non-Federal parties). CRADAs are instruments that may be used in all aspects of a product and/or system life cycle where RDT&E activities occur. The non-Federal parties shall provide funds, personnel, services, facilities, equipment or other resources toward the conduct of specified R&D efforts that are consistent with the missions of the laboratory. The CRADA partners shall share in the intellectual property developed under the effort. The terms of a CRADA may not conform to a procurement contract or cooperative agreement as those terms are used in Sections 6303-6305 of 31 U.S.C.
Core capability	AFPD 63-1, Jul 03	The first fieldable and fully acceptable and supportable initial operational capability delivered to the warfighter.
Counterintelligence	DoD 5200.1-M, Mar 94	Those activities intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations conducted by or on behalf of foreign powers, organizations or persons; it does not include personnel, physical, document, or communications security programs.
Counterintelligence and Security Countermeasures (CI/SCM) Support Element	DoD 5200.1-M, Mar 94	The organizational elements that provide staff-level functional support to program managers in the areas of counterintelligence, security programs and countermeasures, or operations security.
Counterintelligence Support Plan (CISP)	AFPD 63-17, Nov 01	The CISP is a formally coordinated action plan for CI support to protect research and technology at specific DoD research, development, test, and evaluation facilities and acquisition programs. The plan addresses key aspects of the installation, the activity or program, and the nature of the CI activities to be employed. A separate plan may be prepared for each DoD contractor or academic institution where CPI or CSR are involved.
Countermeasure		Action, device, procedure, technique, or other measure that reduces or eliminates one or more vulnerabilities
Countermeasures	DoD 5200.1-M, Mar 94	That form of military science that by employment of devices and/or techniques has as its objective the impairment of the operational effectiveness of enemy activity (JCS Pub 1-02, reference (b)). Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.
Critical Information	DODD 5205.2	Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.
Critical Program Information (CPI) (formerly, Essential Program Information, Technologies, and/or Systems)	DODD 5200.39, Sep 97	Critical program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.
Critical Program Information (CPI) (formerly, Essential Program Information, Technologies, and/or Systems)	DODD 5205.2 DODD 5200.39	Critical program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.
Critical System Resources (CSR)	AFPD 63-17, Nov 01	CSR are those resources, that if unavailable or compromised, could seriously impact development, production, delivery, or operation of a system, component, or technology. An example of a CSR would be a patented chemical compound necessary to a critical production process is produced at a single location. In this example neither the chemical nor the process, but the single manufacturing location and their ability to produce this compound is the CSR.
Data aggregation		The compilation of unclassified individual data systems and data elements resulting in the totality of the information being classified.
Data mining		The analysis of data for relationships that have not previously been discovered

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Defense Acquisition Executive (DAE)	DODD 5000.1	The **Defense Acquisition Executive** (DAE) is the USD(AT&L) who has responsibility for supervising the Defense Acquisition System. The DAE takes precedence on all acquisition matters after the Secretary and the Deputy Secretary.
Defense Acquisition System	DODD 5000.1	The **Defense Acquisition System** is the management process by which the Department of Defense provides effective, affordable, and timely systems to the users.
Defense Agencies	DODD 4630.5	All agencies and offices of the Department of Defense including the Ballistic Missile Defense Organization, the Defense Advanced Research Projects Agency, the Defense Commissary Agency, the Defense Contract Audit Agency, the Defense Finance and Accounting Service, the Defense Information Systems Agency, the Defense Intelligence Agency, the Defense Legal Services Agency, the Defense Logistics Agency, the Defense Threat Reduction Agency, the Defense Security Cooperation Agency, the Defense Security Service, the National Imagery and Mapping Agency, the National Reconnaissance Office, and the National Security Agency.
Defense Information System Network (DISN)	DODD 8500.1	The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations.
Defense-in-Depth	DODD 8500.1	The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness.
Delegation of Disclosure Authority Letter (DDL)		A letter issued by the appropriate designated disclosure authority explaining classification levels, categories, scope, and limitations of information under a DoD Component's disclosure jurisdiction that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate disclosure authorities.
Delegation of Disclosure Authority Letter (DDL)	DoD 5200.1-M, Mar 94	A letter required as part of the Technology Assessment/Control Plan, prepared by the cognizant DoD Component, that provides detailed guidance regarding releasibility of all elements of the system or technology in question. The DDL must be approved by Under Secretary of Defense for Policy (USD(P)) before any promise or release of sensitive technology.
Demilitarized Zone (DMZ)	DODD 8500.1	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. A DMZ is also called a "screened subnet."
Department of State Sensitive But Unclassified (DoS SBU)	DODD 8500.1	Information which originated from the DoS that has been determined to be SBU under appropriate DoS information security polices.
Designated Acquisition Commander (DAC	AFPD 63-1, Jul 03	The individual who performs the same functions as the program executive officer (PEO) on programs that are not assigned to a PEO. Product and Logistic Center commanders and the commander of Air Force Research Laboratory (AFRLs) may be identified as DACs. For acquisition program activities, DACs, like PEOs, are accountable to the AFAE.
Designated Approving Authority (DAA)	DODD 8500.1	The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority (reference (i)).
Designated Disclosure Authority		An official, at subordinate component level, designated by the Head of a DoD Component or the Component's Principal Disclosure Authority to control disclosures of classified military information by his or her organization.
Digital signature		Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation. Same as electronic signature.
Disclosure		Conveying classified information, in any manner, to an authorized representative of a foreign government.
Discretionary access control		Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject. See mandatory access control.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
DISN Designated Approving Authority (DISN DAA)	DODD 8500.1	One of four DAAs responsible for operating the DISN at an acceptable level of risk. The four DISN DAAs are the Directors of DISA, DIA, NSA and the Director of the Joint Staff (delegated to Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)).
DOD 5000 series	CJCSI 3170.01D, Mar 04	DOD 5000 series refers collectively to DODD 5000.1 and DODI 5000.2, references d and e, respectively.
DOD Component	CJCSI 3170.01D, Mar 04	The DOD Components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, DOD Field Activities and all other organizational entities within the Department of Defense.
DoD Components	DoD 5025.1-M	Referred to as "the DoD Components," are identified as the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense.
DoD Directive	DoD 5025.1-M	A DoD issuance that transmits information required by law, the President, or the Secretary of Defense that applies to all branches of the Department of Defense on the way they initiate, govern, or regulate actions. DoD Directives: Establish or describe policy, programs, and organizations. Define missions. Provide authority. Assign responsibilities. Do not prescribe one-time tasks or deadline assignments.
DoD Directives System	DoD 5025.1-M	The single, uniform system that consist of DoD issuances and directive-type memorandums that convey DoD policies, responsibilities, and procedures. It allows the DoD Components to process, review, approve, publish, and distribute DoD issuances efficiently.
DoD Directive-Type Memorandums	DoD 5025.1-M	These are memorandums issued by the Secretary of Defense, the Deputy Secretary of Defense, or the OSD Principal Staff Assistants (PSAs) that are not Deputy Secretary of Defense, or the OSD Principal Staff Assistants (PSAs) that are not published as a DoD issuance because of time constraints. The Secretary or Deputy Secretary of Defense signs directive-type memorandums that promulgate POLICY. OSD PSAs sign directive-type memorandums that promulgate PROCEDURES for implementing policy documents. The office of primary responsibility shall convert a directive-type memorandum into a DoD issuance within 180 days from the date of signature. A copy of the signed memo shall be forwarded to the Director, Directives and Records Division, WHS. The originating office determines who shall coordinate on directive-type memorandums.
DoD Instruction	DoD 5025.1-M	A DoD issuance that implements policies and tells the user how to carry out a policy, operate a program or activity, and assign responsibilities.
DoD Issuances	DoD 5025.1-M	DoD Directives, DoD Instructions, DoD Publications, Administrative Instructions (AIs), and their changes.
DoD Publication		A DoD issuance that implements or supplements DoD Directives and DoD Instructions. DoD Publications provide standard procedures about how users shall manage or operate systems and distribute administrative information. Publications include Catalogs, Directories, Guides, Handbooks, Indexes, Inventories, Lists, Manuals, Modules, Pamphlets, Plans, Regulations, Standards, and Supplements.
DoD Unclassified Controlled Nuclear Information (DoD UCNI)	DODD 8500.1	Unclassified information on security measures (security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83 (reference (ah)). Information is Designated DoD UCNI when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.
Drug Enforcement Administration (DEA)	DODD 8500.1	Sensitive Information. Information originated by the DEA that requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.
Embedded Instrumentation	CJCSI 3170.01D, Mar 04	Data collection and processing capabilities, integrated into the design of a system for one or more of the following uses: diagnostics, prognostics, testing or training.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Enclave	DODD 8500.1	Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in reference (j). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.
Environmental Quality	CJCSI 3170.01D, Mar 04	The condition of the following elements that make up the environment: flora, fauna, air, water, land and cultural resources.
Essential Program Information, Technologies, and/or Systems (EPITS)	DoD 5200.1-M, Mar 94	That information about the program, technologies, and/or systems that if compromised would degrade combat effectiveness or shorten the expected combat-effective life of the system. Access to this information could allow someone to kill, counter or clone the acquisition system before or near scheduled deployment or force a major design change to maintain the same level of effectiveness.
Essential Secrecy	DODD 5205.2	The condition achieved from the denial of critical information to adversaries.
Evolutionary Acquisition	CJCSI 3170.01D, Mar 04	DOD's preferred strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing up-front the need for future capability improvements.
Evolutionary Acquisition (EA)	AFPD 63-1, Jul 03	An acquisition strategy that defines, develops, produces or acquires, and fields an initial hardware or software increment (or block) of operational capability. It is based on technologies demonstrated in relevant environments, time phased requirements, and demonstrated manufacturing or software development capabilities. These capabilities can be provided in a shorter period of time, followed by subsequent increments of capability over time that accommodate improved technology and allowing for full and adaptable systems over time. Each increment will meet a militarily useful capability specified by the user (i.e., at least the thresholds set by the user for that increment); however, the first increment may represent only 60% to 80% of the desired final capability. There are two basic approaches to evolutionary acquisition. In one approach the ultimate functionality can be defined at the beginning of the program, with the content of each deployable increment determined by the maturation of key technologies. In the second approach the ultimate functionality cannot be defined at the beginning of the program, and each increment of capability is defined by the maturation of the technologies matche
Execution Chain	AFPD 63-1, Jul 03	As used in AFPD 63-1, the execution chain is: PM, PEO or DAC or MDA/CAE. Functions as the chain-of-command for program execution.
Executive Council for Modeling and Simulations (EXCIMS)	DODD 5000.59	An organization established by the USD(A&T) and responsible for providing advice and assistance on DoD M&S issues. Membership is determined by the USD(A&T) and is at the Senior Executive Service, flag, and general officer level.
Family of Fystems (FoS)	CJCSI 3170.01D, Mar 04	A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capability needs. The mix of systems can be tailored to provide desired capabilities, dependent on the situation. An example of a FoS would be an anti-submarine warfare FoS consisting of submarines, surface ships, aircraft, static and mobile sensor systems and additional systems. Although these systems can independently provide militarily useful capabilities, in collaboration they can more fully satisfy a more complex and challenging capability: to detect, localize, track, and engage submarines.
Family-of-Systems (FoS)	DODD 4630.5	A set or arrangement of independent systems that can be interconnected or related in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation or mission.
Firewall		System designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in hardware and software, or a combination of both.
For Official Use Only (FOUO)	DODD 8500.1	In accordance with DoD 5400.7-R (reference (af)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (ag)).

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Foreign Disclosure and Technical Information System (FORDTIS)		An automated system to assist decision makers and analysts in reviewing, coordinating, and reaching decisions concerning proposals to release classified military information, materiel, and technology to foreign governments.
Foreign Government Information	DODD 8500.1	Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with reference (o).
Foreign Intelligence Collection Threat	DoD 5200.1-M, Mar 94	The potential of a foreign power, organization, or person to overtly or covertly collect information about U.S. acquisition program technologies, capabilities, and methods of employment that could be used to develop a similar weapon system or countermeasures to the U.S. system or related operations.
Foreign Interest	DODD 5200.39	Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the law of any country other than the United States or its possessions and trust territories; and any person who is not a citizen or national of the United States.
Foreign Interest	DODD 5200.39, Sep 97	Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the law of any country other than the United States or its possessions and trust territories; and any person who is not a citizen or national of the United States.
Functional Area	CJCSI 3170.01D, Mar 04	A broad scope of related joint warfighting skills and attributes that may span the range of military operations. Specific skill groupings that make up the functional areas are approved by the JROC.
Functional Capabilities Board (FCB)	CJCSI 3170.01D, Mar 04	A permanently established body that is responsible for the organization, analysis, and prioritization of joint warfighting capabilities within an assigned functional area.
Functional Capabilities Board Working Group	CJCSI 3170.01D, Mar 04	The FCB Working Groups are the analytic support for the FCBs. They perform the review and assessment of JCIDS documents, work with the sponsors to resolve issues, and make recommendations to the FCB.
Gatekeeper	CJCSI 3170.01D, Mar 04	That individual who makes the initial joint potential designation of JCIDS proposals. This individual will also make a determination of the lead and supporting FCBs for capability proposals. The Gatekeeper is supported in these functions by USJFCOM, J-6, J-7, and the FCB Working Group leads. The Vice Director, J-8 serves as the Gatekeeper.
General-use M&S Applications	DODD 5000.59	Specific representations of the physical environment or environmental effects used by, or common to, many models and simulations; e.g., terrain, atmospheric, or hydrographic effects.
Government Owned/Contractor Operated (GOCO)	AFPD 63-17, Nov 01	An industrial facility owned by the government, but operated by a contractor.
Government-to-Government Channels		The principle that classified information and materiel will be transferred by government officials through official channels or through other channels expressly agreed upon by the governments involved. In either case, the information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.
Granularity		Relative fineness to which an access control mechanism can be adjusted.
HIGH FIDELITY	INTERIM DEFENSE ACQUISITION GUIDEBOOK	Addresses form, fit and function. High-fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting.
Horizontal Protection	DODD 5200.39	The process that ensures CPI associated with more than one acquisition program is protected to the same degree by all involved DoD Components.
Horizontal Protection	DODD 5200.39, Sep 97	The process that ensures CPI associated with more than one acquisition program is protected to the same degree by all involved DoD Components.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
IA Certification and Accreditation	DODD 8500.1	The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.
IA Control		An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with reference (j).
IA Product	DODD 8500.1	Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.
IA-Enabled Information Technology Product	DODD 8500.1	Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.
Inadvertent Disclosure		Accidental exposure of information to a person not authorized access.
Increment	CJCSI 3170.01D, Mar 04	A militarily useful and supportable operational capability that can be effectively developed, produced or acquired, deployed and sustained. Each increment of capability will have its own set of threshold and objective values set by the user.
Increments	AFPD 63-1, Jul 03	A militarily useful and supportable operational capability that can be effectively developed, produced or acquired, deployed, and sustained. Each increment of capability will have its own set of thresholds and objectives set by the user.
Information	DODD 5200.1	Any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of, the Department of Defense.
Information Assurance (IA)	DODD 4630.5 DODD 8500.1	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information Assurance (IA)	CJCSI 3170.01D, Mar 04	Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.
Information Exchange Requirements (IERs)	DODD 4630.5	The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as, why the information is necessary and how that information shall be used.
Information Operations (IO)		Actions taken to affect adversary information and information systems while defending one's own information and information systems.
Information Owner	DODD 8500.1	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Security (INFOSEC)		the system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.
Information Superiority	DODD 4630.5	The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.
Information System (DOD)	DODD 8500.1	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections.
Information System (IS)		The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Information Systems Security		Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.
Information Systems Security Manager (ISSM)		Principal advisor on computer security matters.
Information Systems Security Officer (ISSO)		Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal.
Information Technology (IT)	DODD 4630.5	Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a DoD Component directly, or used by a contractor under a contract with the DoD Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS).
Information Technology (IT)	CJCSI 3170.01D, Mar 04	Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “IT” also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term “IT” does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term “IT” includes National Security Systems (NSS).
Information Technology Architecture (ITA)	DODD 4630.5	An integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the Agency's strategic goals and information resources management goals.
Infrastructure	DoD 5200.1-M, Mar 94	Those items that are used by more than one acquisition program in the pursuit of the development of defense systems. The infrastructure includes laboratories, test facilities, the policy and procedure structure, and education and training organizations.
Initial Capabilities Document (ICD)	CJCSI 3170.01D, Mar 04	Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects and time. The ICD summarizes the results of the DOTMLPF analysis and describes why nonmateriel changes alone have been judged inadequate in fully providing the capability.
Insensitive Munitions	CJCSI 3170.01D, Mar 04	Munitions that minimize the probability of inadvertent initiation and the severity of subsequent collateral damage as a result of unplanned, external stimuli.
Integrated Architecture	DODD 4630.5	An architecture consisting of multiple views or perspectives (operational view, systems view, and technical view) that facilitates integration and promotes interoperability across Family-of-Systems/System-of-Systems and compatibility among related mission area architectures. The operational architecture view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a warfighting function. The systems architecture view is a description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions. The technical architecture view is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Integrated Architecture	CJCSI 3170.01D, Mar 04	An architecture consisting of multiple views or perspectives (operational view, systems view and technical standards view) that facilitates integration, promotes interoperability, and permits identification and prioritization of capability shortfalls and redundancies.
Integrity	DODD 8500.1	Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (reference (i)).
Intelligence		The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.
International Organization		An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.
Internet Protocol (IP)		Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Interoperability	CJCSI 3170.01D, Mar 04	The ability of systems, units or forces to provide data, information, materiel and services to and accept the same from other systems, units or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment.
IT Position Category	DODD 8500.1	Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged) as defined in reference (o). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position.
Joint Capabilities Board (JCB)	CJCSI 3170.01D, Mar 04	The JCB functions to assist the JROC in carrying out its duties and responsibilities. The JCB reviews and, if appropriate, endorses all JCIDS and DOTMLPF proposals prior to their submission to the JROC. The JCB is chaired by the Joint Staff, J-8, Director of Force Structure, Resources, and Assessment. It is comprised of Flag Officer/General Officer representatives of the Services.
Joint Experimentation	CJCSI 3170.01D, Mar 04	An iterative process for developing and assessing concept-based hypotheses to identify and recommend the best value-added solutions for changes in DOTMLPF required to achieve significant advances in future joint operational capabilities.
Joint Functional Concept (JFC)	CJCSI 3170.01D, Mar 04	An articulation of how a future joint force commander will integrate a set of related military tasks to attain capabilities required across the range of military operations. Although broadly described within the Joint Operations Concepts, they derive specific context from the joint operating concepts and promote common attributes in sufficient detail to conduct experimentation and measure effectiveness.
Joint Information		Military information over which two or more DoD components, or two or more Federal Departments or Agencies, exercise control, jurisdiction, or security awareness.
Joint Integrating Concept (JIC)	CJCSI 3170.01D, Mar 04	A JIC describes how a joint force commander integrates functional means to achieve operational ends. It includes a list of essential battlespace effect (including essential supporting tasks, measures of effectiveness, and measures of performance) and a CONOPS for integrating these effects together to achieve the desired endstate.
Joint M&S	DODD 5000.59	Abstract representations of joint and Service forces, capabilities, equipment, materiel, and services used in the joint environment or by two, or more, Military Services.
Joint Mission Areas (JMAs)	DODD 4630.5	JMAs represent a functional group of joint tasks and activities that share a common purpose, and facilitate joint-force operation and interoperability. JMAs provide a logical way to organize the Joint Operational Architecture. JMAs provide the context for defining FoS/SoS relationships sharing a common mission area.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Joint Operating Concept (JOC)	CJCSI 3170.01D, Mar 04	A description of how a future Joint Force Commander will plan, prepare, deploy, employ, and sustain a joint force against potential adversaries' capabilities or crisis situations specified within the range of military operations. Joint Operating Concepts serve as "engines of transformation" to guide the development and integration of joint functional and Service concepts to describe joint capabilities. They describe the measurable detail needed to conduct experimentation, permit the development of measures of effectiveness, and allow decision makers to compare alternatives and make programmatic decisions.
Joint Operational Architecture (JOA)	DODD 4630.5	Description of tasks and activities, operational elements, and information flows required to accomplish or support military operations; defines types of information exchanged, frequency of exchange, which tasks and activities are supported by information exchanges, and nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.
Joint Operations Concepts (JOpsC)	CJCSI 3170.01D, Mar 04	An overarching description of how the future Joint Force will operate across the entire range of military operations. It is the unifying framework for developing subordinate joint operating concepts, joint functional concepts, enabling concepts, and integrated capabilities. It assists in structuring joint experimentation and assessment activities to validate subordinate concepts and capabilities-based requirements.
Joint Potential Designator (JPD)	CJCSI 3170.01D, Mar 04	A designation assigned by the Gatekeeper to specify JCIDS validation, approval and interoperability expectations. a. "JROC Interest" designation will apply to all ACAT I/IA programs and ACAT II and below programs where the capabilities have a significant impacton joint warfighting. This designation may also apply to intelligence capabilities that support DOD and national intelligence requirements. These documents will be staffed through the JROC for validation and approval. All CRDs will be designated as JROC Interest. DOTMLPF change proposals will also be designated as JROC Interest. b. "Joint Integration" designation will apply to ACAT II and below programs where the concepts and/or systems associated with the document do not significantly affect the joint force and an expanded review is not required, but Information Technology and National Security Systems (IT and NSS) interoperability, intelligence or munitions certification is required. Once the required certification(s) are completed, the proposal may be reviewed by the FCB. Joint Integration proposals are validated and approved by the sponsoring Component. c. "Independent" designation will apply to ACAT II and below
Joint Requirements Oversight Council Memorandum (JROCM)	CJCSI 3170.01D, Mar 04	Official JROC correspondence generally directed to an audience(s) external to the JROC. JROCMs are usually decisional in nature.
Joint Systems Architecture (JSA)	DODD 4630.5	The identification and description of all DoD systems and their interconnections necessary to accomplish the tasks and activities described in the Joint Operational Architecture.
Joint Technical Architecture (JTA)	DODD 4630.5	The JTA provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems, and its adoption is mandated for the management, development, and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense.
Key Decision Point (KDP)	CJCSI 3170.01D, Mar 04	The equivalent of a Milestone for space systems.
Key Performance Parameters (KPP)	CJCSI 3170.01D, Mar 04	Those minimum attributes or characteristics considered most essential for an effective military capability. KPPs are validated by the JROC for JROC Interest documents, and by the DOD Component for Joint Integration or Independent documents. CDD and CPD KPPs are included verbatim in the APB.
Key Performance Parameters (KPPs)	DODD 4630.5	Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet a KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a Capstone Requirements Document KPP threshold can be the cause for the FoS/SoS concept to be reassessed or the contributions of the individual systems to be reassessed.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Laboratory and/or Technical Activity	DODI 5535.8, May 99	For the Instruction, that term is, as broadly defined, in 15 U.S.C. 3710a(d)(2)(A) (reference (d)), and shall include the following: 1. "A facility or group of facilities owned, leased, or otherwise used by a Federal Agency, a substantial purpose of which is the performance of research, development, or engineering by employees of the Federal Government." 2. Use of this broad definition, in subdefinition E2.1.3.1., above, is deliberate. That definition is not confined to those DoD Components that are formally titled "laboratories." The intent of that definition is to encompass the wide range of organizations and arrangements that function as laboratories and/or technical activities in DoD research, development, and engineering programs. It shall include laboratories and/or technical activities and reference more diverse arrangements that shall provide a virtual laboratory capability. For example, a DoD Component may have a virtual lab involving a management function accomplished in a Defense Agency activity, plus a dispersed set of research activities to be accomplished by a variety of organizations outside of the sponsoring and/or managing activity. Those capabilities are included in test, logistics, a
Lethality		The ability of a munition or directed-energy weapon to cause damage that will cause the loss or a degradation in the ability of a target system to complete its designated mission(s).
Logistic Support	CJCSI 3170.01D, Mar 04	Logistic support encompasses the logistic services, materiel and transportation required to support the continental United States-based and worldwide-deployed forces.
LOW FIDELITY	INTERIM DEFENSE ACQUISITION GUIDEBOOK	A representative of the component or system that has limited ability to provide anything but first order information about the end product. Low-fidelity assessments are used to provide trend analysis.
Major Automated Information System (MAIS)	AFPD 63-1, Jul 03	An AIS acquisition program that is (1) designated by Assistant Secretary of Defense (Communication, Command, Control and Intelligence) as a MAIS, or (2) estimated to require program costs in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total life-cycle costs in excess of $378 million in FY 2000 constant dollars. MAISs do not include highly sensitive classified programs (as determined by the Secretary of Defense). For the purpose of determining whether an AIS is a MAIS, the following shall be aggregated and considered a single AIS: (1) the separate AISs that constitute a multi-element program; (2) the separate AISs that make up an evolutionary or incrementally developed program; or (3) the separate AISs that make up a multi-component AIS program.
Major Defense Acquisition Program (MDAP)	AFPD 63-1, Jul 03	An acquisition program that is not a highly sensitive classified program (as determine by the Secretary of Defense) and that is designated by the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) as an MDAP, or estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test and evaluation of more than $365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than $2.190 billion in FY 2000 constant dollars.
Malicious code		Software or firmware capable of performing an unauthorized function on an IS.
Mandatory access control		Means of restricting access to objects based on the (MAC) sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. See discretionary access control.
Materiel Solution	DODD 4630.5	Correction of a deficiency, satisfaction of a need, or incorporation of new technology that results in the development, acquisition, procurement or fielding of a new item (including ships, tanks, self-propelled weapons, aircraft, etc., and related software, spares, repair parts and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without disruption as to its application for administrative or combat purposes.
Materiel Solution	CJCSI 3170.01D, Mar 04	A defense acquisition program (nondevelopmental, modification of existing systems, or new program) that satisfies, or is a primary basis for satisfying identified warfighter capabilities. In the case of FoS and SoS approaches, an individual materiel solution may not fully satisfy a necessary capability gap on its own.
Measures of Effectiveness (MOE)	CJCSI 3170.01D, Mar 04	A qualitative or quantitative measure of a system's performance or a characteristic that indicates the degree to which it performs the task or meets a requirement under specified conditions. MOEs should be established to measure the system's capabilities to produce or accomplish the desired result.
Meeting		A conference, seminar, symposium, exhibit, convention, training course, or other gathering during which classified or controlled unclassified information is disclosed.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Milestone Decision Authority	DoD 5200.1-M, Mar 94	The individual designated in accordance with criteria established by the Under Secretary of Defense for Acquisition and Technology to approve entry of an acquisition program into the next phase of the acquisition process.
Milestone Decision Authority (MDA)	AFPD 63-1, Jul 03	The individual designated to authorize or approve the PM's actions and decisions regarding entry of an acquisition program into the next phase of the acquisition process.
Milestone Decision Authority (MDA)	DODD 5000.1	The designated individual with overall responsibility for a program. The MDA shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including Congressional reporting.
Milestone Decision Authority (MDA)	CJCSI 3170.01D, Mar 04	The individual designated, in accordance with criteria established by the USD(AT&L), by the ASD(NII) (for Automated Information System acquisition programs), or by the USecAF (as the DOD Space MDA) to approve entry of an acquisition program into the next phase.
Milestones	CJCSI 3170.01D, Mar 04	Major decision points that separate the phases of an acquisition program.
Militarily Useful Capability	CJCSI 3170.01D, Mar 04	A capability that achieves military objectives through operational effectiveness, suitability and availability, which is interoperable with related systems and processes, transportable and sustainable when and where needed, and at costs known to be affordable over the long term.
Military Department	CJCSI 3170.01D, Mar 04	A department headed by a civilian Secretary appointed by the President and includes a Military Service (the Department of the Navy includes two Services).
Military Departments	DODD 5000.59	The Department of the Army, the Department of the Navy, and the Department of the Air Force, including their National Guard and Reserve components.
Military Services	DODD 5000.59	The Army, the Navy, the Air Force, and the Marine Corps
Military-Use CRADA	DODI 5535.8, May 99	That allows a Federal laboratory and a non-Federal partner to work jointly to assist local businesses by providing limited (4-day maximum) free technical consulting. Preference is given to non-Federal partners that are State organizations, universities, non-profit entities, or business incubators that shall publicize availability of Federal assistance, receive and assess requests for cooperative research, ensure that the laboratory and/or technical activity shall not compete with private organizations, and coordinate work of the laboratory and/or technical activity with the requester companies. The laboratory and/or technical activity shall provide the required assistance and reports to the CRADA partner and the requester company. The requester company only shall provide a problem statement and sign a short 2-page "mini-CRADA" agreement, "subagreement," or "CRADA amendment."
Military-Use CRADA	DODI 5535.8, May 99	A CRADA between a DoD laboratory and/or technical activity and an industrial partner to utilize existing unique capabilities and facilities at the DoD laboratory in a product or process intended primarily for DoD or other military use. Each participant recognizes that it cannot support the research alone nor duplicate existing research or facilities. The technology is incorporated in new DoD systems or products as well as in other commercial opportunities. Specific concerns to be addressed in each military-use CRADA include the following: A CRADA may be the proper vehicle (work is not a contract); Government rights are maintained (not establishing a sole source); Equal opportunity shall be provided to other qualified companies; The laboratory shall not compete with private sector; Preferably, the funds for the laboratory shall not go through industry.
Mission Area Assessment (MAA)	AFPD 63-17, Nov 01	The MAA identifies mission needs using a strategy-to-task process, which links the need for military capabilities to the strategy provided by the Chairman of the Joint Chiefs of Staff (CJCS).
Mission Area Integrated Architectures	DODD 4630.5	Mission area integrated architectures are the common foundation for mission area focused, outcome-based IT and NSS interoperability and supportability processes. Mission area integrated architectures (consisting of operational, systems, and technical views) are derived from JMAs (i.e., subordinate/supporting missions to the JMAs) and/or business/administrative mission areas. Mission area integrated architectures can cover organizational entities (e.g., Joint Task Force, Navy Battle Group or Army Brigade). The Joint Operational Architecture (JOA), the Joint Systems Architecture (JSA) and the Joint Technical Architecture (JTA) serve as the basis for developing mission area integrated architectures.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Mission Area Plan (MAP)	AFPD 63-17, Nov 01	A strategic planning document covering approximately 25 years, the MAP is derived from the Mission Area Assessment and Mission Need Analysis. The MAP records the proposed plan for correcting identified mission deficiencies. It expresses non-materiel solutions, including changes in force structure, system modifications or upgrades, science and technology applications, and new acquisition programs.
Mission Assurance Category (MAC)	DODD 8500.1	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories.
Mission Assurance Category I (MAC I)	DODD 8500.1	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.
Mission Assurance Category II (MAC II)	DODD 8500.1	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.
Mission Assurance Category III (MAC III)	DODD 8500.1	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.
Mission Critical Information Systems (MCIS)	DODD 4630.5	A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act (reference (b)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical should be made by a DoD Component Head, a CINC or their designee.) A Mission Critical Information Technology System has the same meaning as a Mission Critical Information System.
Mission Essential Information Systems (MEIS)	DODD 4630.5	A system that meets the definition of "information system" in the Clinger-Cohen Act (reference (b)), that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission essential should be made by a DoD Component Head, a CINC or their designee.)
Mission Needs Statement (MNS)	AFPD 63-17, Nov 01	A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept and Technology Development Phase of Pre-Systems Acquisition.
Mission Requirements Board	CJCSI 3170.01D, Mar 04	The Mission Requirements Board manages the national requirements process that reviews, validates and approves national requirements for future intelligence capabilities and systems. It is the senior validation and approval authority for future intelligence requirements funded within the National Foreign Intelligence Program (NFIP), and provides advice and council on future requirements funded outside the NFIP.
Misuse detection system		Detector configured to identify behavior that matches a know attack scenario.
Mobile Code	DODD 8500.1	Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.
Model	DODD 5000.59	A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.
MODEL	INTERIM DEFENSE ACQUISITION GUIDEBOOK	A functional form of a system, generally reduced in scale, near or at operational specification. Models will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Modeling and Simulation (M&S) Interoperability	DODD 5000.59	The ability of a model or simulation to provide services to, and accept services from, other models and simulations, and to use the services so exchanged to enable them to operate effectively together.
Modeling and Simulation (M&S) Investment Plan	DODD 5000.59	A DoD plan, published under the authority of the USD(A&T) and with the coordination of the DoD Components, that establishes short-term (present to 6 years) and long-term (beyond 6 years) programs and funding for joint and common use M&S to achieve the specified goals and objectives outlined in the DoD M&S Master Plan.
Modeling and Simulation (M&S) Master Plan	DODD 5000.59	A DoD plan, published under the authority of the USD(A&T) and with the coordination of the DoD Components, that establishes short-term (present to 6 years) and long-term (beyond 6 years) DoD goals and objectives for the application of M&S for joint and common use within the Department of Defense. It shall also include an assessment of current M&S capabilities, a status report on M&S efforts under development, and a road map that delineates the management, investment, and technical strategies required to achieve DoD M&S objectives.
Multi-Discipline Counterintelligence (MDCI) Threat Assessment	DoD 5200.1-M, Mar 94	An assessment made by the cognizant DoD Component that describes those foreign governments, entities, or activities that have the interest and capability to collect information about a system under development.
National Capital Region (NCR)	DoD 5025.1-M	Includes the District of Columbia; Montgomery and Prince George's Counties in Maryland; Arlington, Fairfax, Loudon, and Prince William Counties, and the cities of Alexandria, Fairfax, Falls Church, Manassas, and Manassas Park in Virginia.
National Information Assurance Partnership (NIAP)	DODD 8500.1	Joint initiative between NSA and NIST responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.
National Security	DODD 5200.1	The national defense or foreign relations of the United States.
National Security System (NSS)	DODD 4630.5	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 40 U.S.C. Section 1452, Information Technology Management Reform Act of 1996.)
National Security Systems (NSS)	CJCSI 3170.01D, Mar 04	Telecommunications and information systems, operated by the DOD -- the functions, operation or use of which involves (1) intelligence activities, (2) cryptologic activities related to national security, (3) the command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications).
Need-to-Know	DODD 8500.1	Necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties (reference (i) modified).
Need-to-Know Determination	DODD 8500.1	Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (i)).

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Net-Ready Key Performance Parameter (NR-KPP)	CJCSI 3170.01D, Mar 04	The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements: •Compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM) •Compliance with applicable GIG Key Interface Profiles (KIPs) •Verification of compliance with DOD information assurance requirements •Supporting integrated architecture products required to assess information exchange and use for a given capability nonmateriel Solution - Changes in doctrine, organization, training, leadership education, personnel or facilities to satisfy identified functional capabilities.
Non-Materiel Solution	DODD 4630.5	Changes in doctrine, organization, training, leadership, personnel or facilities that satisfy identified mission needs.
Nonprofit Institution	DODI 5535.8, May 99	That is an organization owned and operated exclusively for scientific or educational purposes, the net earnings of which shall not benefit any private shareholder or individual.
Non-repudiation	DODD 8500.1	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (reference (i)).
Objective Value	CJCSI 3170.01D, Mar 04	The desired operational goal associated with a performance attribute, beyond which any gain in utility does not warrant additional expenditure. The objective value is an operationally significant increment above the threshold. An objective value may be the same as the threshold when an operationally significant increment above the threshold is not significant or useful.
Office of the Secretary of Defense (OSD)	DoD 5025.1-M	The principal staff element used by the Secretary and Deputy Secretary of Defense to exercise authority, direction, and control over the Department of Defense. The OSD shall include the: Immediate Offices of the Secretary and Deputy Secretary ofDefense. Under Secretaries of Defense (USDs). Director of Defense Research and Engineering (DDR&E). Assistant Secretaries of Defense (ASDs). General Counsel of the Department of Defense (GC, DoD). Inspector General of the Department of Defense (IG DoD). Director of Operational Test and Evaluation (DOT&E). Assistants to the Secretary of Defense (ATSDs). OSD Directors or equivalents who report directly to the Secretary or Deputy Secretary of Defense.
Office of the Secretary of Defense (OSD)	DODD 5000.59	Includes the immediate Offices of the Secretary and Deputy Secretary of Defense, the Under Secretaries of Defense, the Comptroller of the Department of Defense (C, DoD), the Director of Defense Research and Engineering (DDR&E) (reference (l)), the Assistant Secretaries of Defense (ASDs), the General Counsel of the Department of Defense (GC, DoD), the Assistants to the Secretary of Defense (ATSDs), the OSD Directors, or equivalents, who report directly to the Secretary or the Deputy Secretary of Defense, and such other staff offices as the Secretary of Defense establishes to assist in carrying out assigned responsibilities.
Official DoD Information	DODD 8500.1	All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department (reference (s)).
Operational Concept	DODD 4630.5	An end-to-end stream of activities that defines how force elements, systems, organizations, and tactics combine to accomplish a military task.
Operational Effectiveness	CJCSI 3170.01D, Mar 04	Measure of the overall ability to accomplish a mission when used by representative personnel in the environment planned or expected for operational employment of the system considering organization, doctrine, tactics, supportability, survivability, vulnerability and threat.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
OPERATIONAL ENVIRONMENT	INTERIM DEFENSE ACQUISITION GUIDEBOOK	Environment that addresses all of the operational requirements and specifications required of the final system to include platform/packaging.
Operational Requirements Document (ORD)	AFPD 63-17, Nov 01	A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or the user's representative at each milestone beginning with Milestone Bsystem Development and Demonstration of the Systems Acquisition process. (Replaced with the ICD, CDD, and CDP)
Operational Suitability	CJCSI 3170.01D, Mar 04	The degree to which a system can be placed and sustained satisfactorily in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, habitability, manpower, logistics, supportability, logistics supportability, natural environment effects and impacts, documentation and training requirements.
Operations Security (OPSEC)	DODD 5205.2	For the DoD Components, OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to: dentify those actions that may be observed by adversary intelligence systems. Determine what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
Operations Security (OPSEC)	DoD 5200.1-M, Mar 94	A process of analyzing friendly actions attendant to military operations and other activities to: 1. dentify those actions that can be observed by adversary intelligence systems. 2. Determine the indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. 3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
Operator	CJCSI 3170.01D, Mar 04	An operational command or agency that employs the acquired system for the benefit of users. Operators may also be users.
OPSEC Process	DODD 5205.2	The OPSEC process is an analytical, risk-based process that incorporates five distinct elements: Identifying critical information; Analyzing threats; Analyzing vulnerabilities; Assessing risks; and Applying countermeasures. The OPSEC process examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by potential adversaries.
Organizational Charter	DoD 5025.1-M	A DoD Directive that establishes the responsibilities, functions, relationships, and delegated authorities, as applicable, of a OSD Principal Staff Assistant, Defense Agency, DoD Field Activity, DoD Executive Agent, or other organizational entity in the Department of Defense.
Originating DoD Component		The DoD Agency that exercises original classification jurisdiction for classified information.
OSD Principal Staff Assistants (PSAs)	DoD 5025.1-M	The Under Secretaries of Defense, the Director of Defense Research and Engineering, the Assistant Secretaries of Defense, the General Counsel of the Department of Defense, the Inspector General of the Department of Defense, the Director of Operational Test and Evaluation, the Assistants to the Secretary of Defense, certain Deputy Under Secretaries of Defense, and OSD Directors or equivalents who report directly to the Secretary or Deputy Secretary of Defense.
Other Organizational Entities in the Department of Defense	DoD 5025.1-M	Organizations established under the Secretary's authority in 10 U.S.C. 113 or 125 (reference (b)), but excluding those designated under Section 191 of reference (c)). Those organizations include, but are not limited to, the Uniformed Services University of the Health Sciences (USUHS) and the National Reconnaissance Office (NRO).

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Outcome-Based Interoperability	DODD 4630.5	An interoperability process that: Includes experts from the operational community to identify, consolidate and prioritize interoperability deficiencies; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities. Characterizes IT and NSS interoperability requirements in a family-of-systems or system-of-systems mission area context and relates IT and NSS through integrated architectures derived from the Joint Operational Architecture and associated Joint Mission Areas. Precisely defines operational user requirements to include interoperability as a Key Performance Parameter. Incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership, personnel, or facilities) solutions. Verifies solution sets in formal tests or operational exercises. Continuously evaluates interoperability Key Performance Parameters and verifies overall IT and NSS interoperability throughout a system's life.
Outsourced IT-based Process	DODD 8500.1	For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.
Platform IT Interconnection	DODD 8500.1	For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.
Portfolio	DODD 8500.1	The aggregate of IT investments for DoD information systems, infrastructure and related technical activities that are linked to mission goals, strategies, and architectures, using various assessment and analysis tools to permit information and IT decisions to be based on their contribution to the effectiveness and efficiency of military missions and supporting business functions. Portfolios enable the Department of Defense to manage IT resources and align strategies and programs with Defense-wide, functional, and organizational goals and measures.
Principal Staff Assistants (PSAs)	DODD 5000.59	The Under Secretaries of Defense; the C, DoD; the DDR&E; the ASDs; the Inspector General of the Department of Defense; the GC, DoD; the ATSDs; and the OSD Directors, or equivalents, who report directly to the Secretary or Deputy Secretary of Defense.
Privacy Data	DODD 8500.1	Any record that is contained in a system of records, as defined in the reference (ad) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.
Private Key		Encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret.
Privileged Access		Explicitly authorized access of a specific user, process, or computer to a computer resource(s).
Program Executive Officer (PEO)	AFPD 63-1, Jul 03	A military or civilian official who has primary responsibility for directing several MDAPs and assigned major system and non-major system acquisition programs. A PEO has no other command or staff responsibilities within the USAF and only reports to and receives guidance and direction from the AFAE.
Program Information	DoD 5200.1-M, Mar 94	For the purposes of this program (DoD5200.1-M), information that includes programmatic data and/or information and weapons system, subsystem, or component information.
Program Management Directive (PMD)	AFPD 63-17, Nov 01	The official Air Force document used to direct acquisition responsibilities to the appropriate major commands, agencies, program executive office, or designated acquisition commander. All acquisition programs require PMDs.
Program Manager (PM)	AFPD 63-1, Jul 03	As used in AFPD 63-1, applies collectively to System Program Director, single manager, or acquisition program manager.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Program Manager (PM)	DODD 5000.1	The **Program Manager** (PM) is the designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for credible cost, schedule, and performance reporting to the MDA.
Program Protection	DoD 5200.1-M, Mar 94	The safeguarding of defense systems and technical data anywhere in the acquisition process to include the technologies being developed, the support systems (e.g., test and simulation equipment), and research data with military applications. This protection activity involves integrating all security disciplines, counterintelligence, and other defensive methods to protect the essential program information, technologies, and systems data from intelligence collection and unauthorized disclosure.
Program Protection Plan (PPP)	DODD 5200.39	A comprehensive plan to safeguard critical program and technology information that is associated with a defense acquisition program. The level of detail and complexity of the PPP will vary based on the criticality of the program or system, the CPI, and the phase of the acquisition process being addressed.
Program Protection Plan (PPP)	DoD 5200.1-M, Mar 94	A comprehensive protection and technology control management plan established for each defense acquisition program to identify and protect classified and other sensitive information from foreign intelligence collection or unauthorized disclosure. (The PPP is designed to negate the Program Protection Threats and Vulnerabilities.)
Program Protection Plan (PPP)	DODD 5200.39, Sep 97	A comprehensive plan to safeguard critical program and technology information that is associated with a defense acquisition program. The level of detail and complexity of the PPP will vary based on the criticality of the program or system, the CPI, and the phase of the acquisition process being addressed.
Program Protection Planning	AFPD 63-17, Nov 01	An acquisition and logistics managed program process that identifies asystem's critical program elements, threats, and vulnerabilities throughout the system's life-cycle. Program Protection Planning is a comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes. through the integration of embedded system security processes, security manpower, equipment, and facilities.
Program Protection Survey	DoD 5200.1-M, Mar 94	A survey, conducted during each acquisition phase, to assess the effectiveness of the countermeasures prescribed in the program protection plan at a specific point in time.
Program Protection Threats	DoD 5200.1-M, Mar 94	The program protection threats include life-cycle protection threats, foreign intelligence collection efforts, and unauthorized disclosure of essential program information, technologies, and systems during the acquisition process.
Proprietary	DODD 8500.1	Information that is provided by a source or sources under the condition that it not be released to other sources.
PROTOTYPE	INTERIM DEFENSE ACQUISITION GUIDEBOOK	A physical or virtual model used to evaluate the technical or manufacturing feasibility or military utility of a particular technology or process, concept, end item or system.
Proxy	DODD 8500.1	Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.
Public Domain Software	DODD 8500.1	Software not protected by copyright laws of any nation that carries no warranties or liabilities, and may be freely used without permission of or payment to the creator.
Public Information	DODD 8500.1	Official DoD information that has been reviewed and approved for public release by the information owner in accordance with reference (s).
Public Key Infrastructure (PKI)		Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.
Recoverability		Following combat damage, the ability to take emergency action to prevent loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities. Recoverability is considered a subset of survivability.
RELEVANT ENVIRONMENT	INTERIM DEFENSE ACQUISITION GUIDEBOOK	Testing environment that simulates the key aspects of the operational environment.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Research and Technology	DODD 8500.1	Activities that may be described as basic research, applied research, and advanced technology development, demonstrations or equivalent activities, regardless of budget activity. Definitions for Basic Research, Applied Research and Advanced Technology Development are provided in the DoD FMR, Chapter 5 (reference (ac)).
Risk Management	DoD 5200.1-M, Mar 94	The comparison and analysis of the relative threat (intent and capability to collect the information); the vulnerability of the asset; the cost and administrative burden of possible countermeasures; and the value of the asset used to determine the appropriate level of protection to control and reduce the risk of compromise or disclosure to acceptable levels. Risk management allows the acceptance of risk in the security process based upon a cost-benefit analysis.
Risk Management	DODD 5200.39	An organized, analytical process of identifying vulnerabilities, quantifying and assessing associated risks, and implementing and/or controlling the appropriate approach for preventing or handling each risk identified.
Risk Management	DODD 5200.39, Sep 97	An organized, analytical process of identifying vulnerabilities, quantifying and assessing associated risks, and implementing and/or controlling the appropriate approach for preventing or handling each risk identified
Risk Management		Process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.
Robustness	DODD 8500.1	A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. The Department of Defense has three levels of robustness
Robustness (Basic)	DODD 8500.1	Security services and mechanisms that equate to good commercial practices.
Robustness (High)	DODD 8500.1	Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.
Robustness (Medium)	DODD 8500.1	Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.
Security Assurance		The written confirmation, requested by and exchanged between governments, of the security clearance level or eligibility for clearance, of their employees, contractors, and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of U.S. classified military information possesses the requisite security clearance and is approved by his or her government for access to information of the security classification involved on behalf of the foreign government and that the recipient will comply with any security requirements specified by the United States. In the case of industrial facilities, the security assurance should include a statement concerning the level of storage capability.
Security Domain	DODD 8500.1	Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and in its connection to other classified or unclassified information systems.
Sensitive But Unclassified (SBU)	DODD 8500.1	A term commonly and inappropriately used within the Department of Defense as a synonym for Sensitive Information, which is the preferred term.
Sensitive Compartmented Information (SCI)	DODD 8500.1	Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.
Sensitive Compartmented Information (SCI)	AFPD 63-17, Nov 01	All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DoD 5200.1-R, *Information Security Progra* m.)
Sensitive Information	DoD 5200.1-M, Mar 94	Any information, the loss, misuse, or unauthorized access to which would or could adversely affect the organizational and/or national interest but which does not meet classification criteria specified in DoD 5200.1-R

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Sensitive Information	DODD 8500.1	Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code, "The Privacy Act" (reference (ad)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of Title 15, United States Code, "The Computer Security Act of 1987" (reference (ae)).) This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to the following: FOUO (For Official Use Only) Privacy Data DoD Unclassified Controlled Nuclear Information (DoD UCNI) Unclassified Technical Data Proprietary Foreign Government Information Department of State Sensitive But Unclassified (DoS SBU) Drug Enforcement Administration (DEA) Sensitive Information
SIMULATED OPERATIONAL ENVIRONMENTAL	INTERIM DEFENSE ACQUISITION GUIDEBOOK	Either 1) a real environment that can simulate all of the operational requirements and specifications required of the final system, or 2) a simulated environment that allows for testing of a virtual prototype; used in either case to determine whether a developmental system meets the operational requirements and specifications of the final system.
Simulation	DODD 5000.59	A method for implementing a model over time. Also, a technique for testing, analysis, or training in which real-world systems are used, or where real-world and conceptual systems are reproduced by a model.
Single Manager (SM)	AFPD 63-1, Jul 03	The single face to the customer for a system or product group. The SM directs one or more programs and is accountable to the PEO or the DAC. The SM is vested with full authority, responsibility and resources to execute a program on behalf of the Air Force.
Single Manager (SM)	AFPD 63-17, Nov 01	A military department of agency designated by the Secretary of Defense to be responsible for management of specified commodities or common service activities on a Department of Defense-wide basis.
Special Access Program	DoD 5200.1-M, Mar 94	Any program imposing need-to-know or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Examples of such controls include, but are not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine need to know; or special lists of persons determined to have a need-to-know.
Special Access Program (SAP)	AFPD 63-17, Nov 01	A sensitive program, approved in writing by a head of agency with original top secret authority, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program.
Spiral Development	AFPD 63-1, Jul 03	Spiral Development is an iterative process for developing a defined set of capabilities within an increment, providing opportunity for interaction between the warfighter, technologist, developer, sustainer, and tester communities to refine the requirements, provide continuous feedback and provide the best possible capability within that and subsequent increments. The spiral development process is an iterative set of sub-processes which may include: establishing performance objectives; designing; coding/fabricating/integrating; experimenting; testing; assessing operational utility; making tradeoffs; and delivering. Other sub processes may be added as needed. Spiral development characteristics include: a team of stakeholders motivated to collaborate and mitigate risk; a development plan and decision process; a process to refine requirements; a firm schedule per increment; continued negotiation of performance and cost goals; test/experimentation; and a warfighter decision to field, continue development, or terminate any portion of the increment. Experimentation, which includes simulation and exercises, allows all concept stakeholders to solidify their understanding of a concept beyond paper studies or ideas. When strung together, spirals facilitate more precise and rapid maturation of new technologies and refinement of war
Sponsor	CJCSI 3170.01D, Mar 04	The DOD component responsible for all common documentation, periodic reporting and funding actions required to support the capabilities development and acquisition process for a specific capability proposal.
Strategic War Plan		A plan for the overall conduct of a war

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Supportability	DODD 4630.5	The ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain design, development, testing, training, or operations of the IT or NSS to its required capability.
Supporting IA Infrastructures	DODD 8500.1	Collections of interrelated processes, systems, and networks that provide a continual flow of information assurance services throughout the Department of Defense, e.g., the key management infrastructure or the incident detection and response infrastructure.
Surface Passivation		A very thin caoting to exclude oxygen and moisture from contact with the components
Survivability		The capability of a system and crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. Survivability consists of susceptibility, vulnerability, and recoverability.
Susceptibility		The degree to which a weapon system is open to effective attack due to one or more inherent weakness. (Susceptibility is a function of operational tactics, countermeasures, probability of enemy fielding a threat, etc.) Susceptibility is considered a subset of survivability.
Sustainability	CJCSI 3170.01D, Mar 04	The ability to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materiel and consumables necessary to support military effort.
Sustainment	CJCSI 3170.01D, Mar 04	The provision of personnel, logistic and other support required to maintain and prolong operations or combat until successful accomplishment or revision of the mission or of the national objective.
System Administrator (SA)		Individual responsible for the installation and maintenance of an information system, providing effective IS utilization, adequate security parameters, and sound implementation of established INFOSEC policy and procedures.
System Decomposition	DoD 5200.1-M, Mar 94	The separation of the major mission functions and capabilities of the system and then identifying those components or technologies that give the system this ability.
System of Systems (SoS)	CJCSI 3170.01D, Mar 04	A set or arrangement of interdependent systems that related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. An example of a SoS could be interdependent information systems. While individual systems within the SoS may be developed to satisfy the peculiar needs of a given user group (like a specific Service or agency), the information they share is so important that the loss of a single system may deprive other systems of the data needed to achieve even minimal capabilities.
System Program Director (SPD	AFPD 63-1, Jul 03	A single manager who directs a weapon system program and manages the system program office. The SPD is the program manager vested with full authority, responsibility and resources to execute an approved acquisition program on behalf of the Air Force.
System Program Office (SPO)	AFPD 63-17, Nov 01	The office of the SM and the single point of contact with industry, government agencies, and all other life-cycle activities throughout the systems acquisition and sustainment processes.
System Security Engineering (SSE)	DoD 5200.1-M, Mar 94	An element of system engineering that applies scientific and engineering principles to identify and reduce system susceptibility to damage, compromise, or destruction; the identification, evaluation, and elimination or containment of system vulnerabilities to known or postulated security threats in the operational environment.
System Security Management Plan	DoD 5200.1-M, Mar 94	A formal document that fully describes the planned security tasks required to meet system security engineering requirements, including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering, design and management activities, and related systems.
System Threat	DoD 5200.1-M, Mar 94	The threat to be countered by the defense system being acquired.
System Threat Assessment Report (STAR)	DoD 5200.1-M, Mar 94	The basic authoritative threat assessment, tailored for and focused on, a particular (i.e., single) U.S. major defense system. It describes the threat to be countered in the projected threat environment. The threat information should reference DIA-validated documents. Technology. 1. The information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves. (Export Administration Act of 1979, as amended in 1981, 1985 and 1988.) 2. The technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software. The term does not include the goods themselves. (DoD Directive 2040.2)

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Technical Assistance	DODI 5535.8, May 99	Allows a Federal laboratory and a non-Federal partner to work jointly to assist local businesses by providing limited (up to 4-day maximum) free technical consulting. Preference shall be given to non-Federal partners that are State organizations, universities, or non-profit entities, including the FLC, which shall publicize availability of Federal assistance, ensure that the laboratory and/or technical activity shall not compete with private organizations, and coordinate the work of the laboratory and/or technical activity with the requester companies. The laboratory and/or technical activity shall provide the required assistance in the form of technical information, lessons, learned, problem solving, or further advice. At no time are technical assistance activities or technical assistance CRADAs to be used to accomplish R&D.
Technical Assistance CRADA	DODI 5535.8, May 99	An agreement between one or more Federal laboratories and/or technical activities and one or more non-Federal parties. Under a CRADA, the Government laboratories and/or technical activities shall provide personnel, services, facilities, equipment or other resources with or without reimbursement (but not funds to the non-Federal parties). CRADAs are instruments that may be used in all aspects of a product and/or system life cycle where RDT&E activities occur. The non-Federal parties shall provide funds, personnel, services, facilities, equipment or other resources toward the conduct of specified R&D efforts that are consistent with the missions of the laboratory. The CRADA partners shall share in the intellectual property developed under the effort. The terms of a CRADA may not conform to a procurement contract or cooperative agreement as those terms are used in Sections 6303-6305 of 31 U.S.C.
Technical Directorate Director (TDD)	AFPD 63-17, Nov 01	The Air Force Research Laboratory (AFRL) is one laboratory made up of multiple technical directorates. Each technical directorate is led by a single "Director," who is responsible for the technology programs that occur at their particular directorate.
Technology Assessment and Control Plan	DODD 5200.39	The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and, the development of access controls and measures necessary to protect the U.S. technological or operational advantage of the system, as prescribed in DoD Directive 5230.11 (reference (m)) and DoD Directive 5530.3 (reference (p)).
Technology Assessment and Control Plan	DODD 5200.39, Sep 97	The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and, the development of access controls and measures necessary to protect the U.S. technological or operational advantage of the system, as prescribed in DoD Directive 5230.11 (reference (m)) and DoD Directive 5530.3 (reference (p))
Technology Assessment/Control Plan (TA/CP)	DoD 5200.1-M, Mar 94	The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and the development of access controls and protective measures as necessary to protect the U.S. technological or operational advantage represented by the system.
Technology Protection Plan (TPP)	AFPD 63-17, Nov 01	Similar to the PPP developed in the acquisition cycle, a TPP is developed by research organizations that identify CPI or CSR requiring increased protection.
TECHNOLOGY READINESS LEVELS (TRL)		The following matrix lists the various technology readiness levels and descriptions from a systems approach for both HARDWARE and SOFTWARE. DoD Components may provide additional clarifications for Software. Supplemental definitions follow the table.
Technology Transfer	DoD 5200.1-M, Mar 94	Transferring, exporting, or disclosing defense articles, defense service, or defense technical data covered by the U.S. Munitions List to any foreign person or entity in the United States or abroad.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Technology Transfer (T2)	DODI 5535.8, May 99	The intentional communication (sharing) of knowledge, expertise, facilities, equipment, and other resources for application to military and nonmilitary systems. Domestic T2 activities shall include the following: 1. Spin-off activities that shall demonstrate DoD technology; e.g., commercial viability of technologies already developed or presently being developed for U.S. security purposes. The primary purpose of those activities, which encompass T2, shall be to promote and make available existing DoD-owned or –developed technologies and technical infrastructure to a broad spectrum of non-DoD applications. 2. Dual-use science and technology and other activities that develop technologies that have both DoD and non-DoD applications. 3. Spin-on promotion activities that shall demonstrate the U.S. security utility of technologies developed outside of the Department of Defense. That goal shall be to incorporate the innovative technology into military systems to meet mission needs at a lower acquisition cost by taking advantage of the economies of scale by purchasing from a larger industrial base.
Telework		Any arrangement in which an employee performs officially assigned duties at an alternative worksite on either a regular and recurring, or on an ad hoc, basis (not including while on official travel).
Threat	DoD 5200.1-M, Mar 94	The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate U.S. mission accomplishment or reduce force, system, or equipment effectiveness.
Threshold Value	CJCSI 3170.01D, Mar 04	A minimum acceptable operational value below which the utility of the system becomes questionable.
Time- or Event-Phased Classification Guide	DoD 5200.1-M, Mar 94	The adaptation of the DoD security classification guide to the acquisition process addressing the essential program information, technologies, or systems and the associated subsystems and technologies during each phase of the acquisition process. The guide indicates classification or sensitivity and the date or event that will cause a change to the level of the classification or sensitivity.
Traps		A preset event or reaction that is directly triggered by tampering or inspection
Unclassified Technical Data	DODD 8500.1	Data that is not classified, but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25 (reference (ai)).
Universal Reference Resources (URRs)	DODD 4630.5	Reference models and information standards, which serve as sources for guidelines and attributes that must be consulted while building integrated architecture products. The following are the currently listed URRs: DoD Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture Framework; C4ISR Core Architecture Data Model; Defense Data Dictionary, Levels of Information Systems Interoperability; Universal Joint Task List; Joint Operational Architecture; Technical Reference Model; Defense Information Infrastructure Common Operating Environment; Shared Data Environment; and the DoD Joint Technical Architecture.
User	CJCSI 3170.01D, Mar 04	An operational command or agency that receives or will receive benefit from the acquired system. Combatant commanders and their Service Component commands are the users. There may be more than one user for a system. Because the Service Component commands are required to organize, equip and train forces for the combatant commanders, they are seen as users for systems. The Chiefs of the Services and heads of other DOD Components are validation and approval authorities and are not viewed as users.
User Representative	CJCSI 3170.01D, Mar 04	A command or agency that has been formally designated to represent single or multiple users in the capabilities and acquisition process. The Services and the Service Components of the combatant commanders are normally the user representatives. There should only be one user representative for a system.
Validation	DODD 5000.59	The process of determining the degree to which a model is an accurate representation of the real-world from the perspective of the intended uses of the model.
Validation	CJCSI 3170.01D, Mar 04	The review of documentation by an operational authority other than the user to confirm the operational capability. Validation is a precursor to approval.
Validation Authority	CJCSI 3170.01D, Mar 04	The individual within the DOD Components charged with overall capability definition and validation. The Vice Chairman of the Joint Chiefs of Staff, in the role as the Chairman of the JROC, is the Validation Authority for all potential major defense acquisition programs. The Validation Authority for JCIDS issues is dependent upon the JPD of the program or initiative as specified below: a. JROC Interest - The JROC is the Validation Authority. b. Joint Integration - The sponsor is the Validation Authority. c. Independent - The sponsor is the Validation Authority.

DEFINITIONS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Name	Reference	Definition
Verification	DODD 5000.59	The process of determining that a model implementation accurately represents the developer's conceptual description and specifications.
Vulnerability		The characteristic of a system that causes it to suffer a definite degradation (loss or reduction of capability to perform its designated mission) as a result of having been subjected to a certain (defined) level of effects in an unnatural (man-made) hostile environment. Vulnerability is considered a subset of survivability.
Vulnerability	DoD 5200.1-M, Mar 94	The susceptibility of systems or components to the threat in a given environment.
Warfighter	AFPD 63-1, Jul 03	As used in AFPD63-1, the individual(s)/organizations previously identified in various acquisition and requirements publications as the “user” or “customer.” Ultimately all materiel, services, hardware/software, and systems developed and procured directly or indirectly support the joint warfighting mission of the United States Air Force, therefore; the warfighter is and must remain the focus of the acquisition, technology, testing, budgeting, sustainment, and other participating communities.

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
ACAT	CJCSI 3170.01D, Mar 04	acquisition category
ACAT	Interim Defense Acquisition Guidebook DoD 5200.1-M	Acquisition Category
ACE	AFPD 63-1, Jul 03	Acquisition Center of Excellence
Acronym	Reference	Definition
ACSA	Interim Defense Acquisition Guidebook	Acquisition Cross-Servicing Agreement
ACTD	CJCSI 3170.01D, Mar 04	advanced concept technology demonstration
ADL		Advanced Distributed Learning
ADM	Interim Defense Acquisition Guidebook	Acquisition Decision Memorandum
AFAE	AFPD 63-1, Jul 03	Air Force Acquisition Executive
AFFARS	AFPD 63-1, Jul 03	Air Force Federal Acquisition Regulation Supplement
AFI	AFPD 63-1, Jul 03	Air Force Instruction
AFOSI	DoD 5200.1-M	Air Force Office of Special Investigations
AFPD	AFPD 63-1, Jul 03	Air Force Policy Directive
AFRC	AFPD 63-1, Jul 03	Air Force Reserve Command
AFRL	AFPD 63-1, Jul 03	Air Force Research Laboratory
AI		Administrative Instruction
AIS	DoD 5200.1-M	Automated Information System
ANACI		Access national Agency Check with Written Inquiries
ANSI	Interim Defense Acquisition Guidebook	American National Standards Institute
Anti-Tamper Techniques		Systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems
AoA	CJCSI 3170.01D, Mar 04	analysis of alternatives
APB	CJCSI 3170.01D, Mar 04	acquisition program baseline
APB	Interim Defense Acquisition Guidebook	Acquisition Program Baseline
APUC	Interim Defense Acquisition Guidebook	Average Procurement Unit Cost

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
ASD(AT&L)		Assistant Secretary of Defense (Acquisition & Technology)
ASD(C3I)	AT Implementation Guidelines, USD, May 00	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASD(C3I)	Interim Defense Acquisition Guidebook DoD 5200.1-M	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence
ASD(HA)	CJCSI 3170.01D, Mar 04	Assistant Secretary of Defense (Health Affairs)
ASD(NII)	CJCSI 3170.01D, Mar 04	Assistant Secretary of Defense for Networks and Information Integration
ASPP		Acquisition Systems Protection Program
AT	AT Implementation Guidelines, USD, May 00	Anti-Tamper techniques
AT		Anti-Tamper
AT&L	CJCSI 3170.01D, Mar 04	acquisition, technology and logistics
ATS	Interim Defense Acquisition Guidebook	Automatic Test System
BES	Interim Defense Acquisition Guidebook	Budget Estimate Submission
C/SSR	Interim Defense Acquisition Guidebook	Cost/Schedule Status Report
C3I/S&IO		Command, Control, Communications, and Intelligence, Security & Information Operations
C4I	CJCSI 3170.01D, Mar 04	command, control, communications, computers and intelligence
C4ISP	Interim Defense Acquisition Guidebook	Command, Control, Communications, Computers, and Intelligence Support Program
C4ISR	AT Implementation Guidelines, USD, May 00	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C4ISR	Interim Defense Acquisition Guidebook	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAE	Interim Defense Acquisition Guidebook	Component Acquisition Executive

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
CAIG	Interim Defense Acquisition Guidebook	Cost Analysis Improvement Group
CAIV	Interim Defense Acquisition Guidebook	Cost as an Independent Variable
CARD	Interim Defense Acquisition Guidebook	Cost Analysis Requirements Description
CARS	Interim Defense Acquisition Guidebook	Consolidated Acquisition Reporting System
CCDR	Interim Defense Acquisition Guidebook	Contractor Cost Data Reporting
CDD	CJCSI 3170.01D, Mar 04	Capability Development Document
CERT		Computer Emergency response Team
CFSR	Interim Defense Acquisition Guidebook	Contract Funds Status Report
CI		counterintelligence
CINC	Interim Defense Acquisition Guidebook	Commander-in-Chief
CIO	CJCSI 3170.01D, Mar 04	chief information officer
CJCS	CJCSI 3170.01D, Mar 04	Chairman of the Joint Chiefs of Staff
CJCS	Interim Defense Acquisition Guidebook	Chairman of the Joint Chiefs of Staff
CJCSI		Chairman of the Joint Chiefs of Staff Instruction
CJCSI	CJCSI 3170.01D, Mar 04	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	CJCSI 3170.01D, Mar 04	Chairman of the Joint Chiefs of Staff Manual
CMDS		Computer Misuse Detection System
COCO	AFPD 63-17, Nov 01	Contractor Owned Contractor Operated
COCOM	CJCSI 3170.01D, Mar 04	combatant command
COI	Interim Defense Acquisition Guidebook	Critical Operational Issue
COMSEC		Communications Security
COP	CJCSI 3170.01D, Mar 04	common operational picture

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
COTS	Interim Defense Acquisition Guidebook	Commercial, Off-the-Shelf
CPD	CJCSI 3170.01D, Mar 04	Capability Production Document
CPI	Interim Defense Acquisition Guidebook	Critical Program Information
CPR	Interim Defense Acquisition Guidebook	Cost Performance Report
CRD	Interim Defense Acquisition Guidebook	Capstone Requirements Document
CRD	CJCSI 3170.01D, Mar 04	Capstone Requirements Document
CSAF	AFPD 63-1, Jul 03	Chief of Staff of the Air Force
CWP	Interim Defense Acquisition Guidebook	Coalition Warfare Program
D, PA&E	CJCSI 3170.01D, Mar 04	Director, Program Analysis and Evaluation
D,S&TS	Interim Defense Acquisition Guidebook	Director, Strategic and Tactical Systems
DAA		Designated Approving Authority
DAB	CJCSI 3170.01D, Mar 04	Defense Acquisition Board
DAB	Interim Defense Acquisition Guidebook	Defense Acquisition Board
DAC	Designated Acquisition Commander	Designated Acquisition Commander
DAE	AFPD 63-1, Jul 03	Defense Acquisition Executive
DAES	Interim Defense Acquisition Guidebook	Defense Acquisition Executive Summary
DAPSG	Interim Defense Acquisition Guidebook	Defense Acquisition Policy Steering Group
DARPA		Defense Advanced Research Projects Agency
DASD(I)		Deputy Assistant Secretary of Defense (Intelligence)
DCI		Director of Central Intelligence
DCII		Defense Central and Investigations Index (DCII)

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
DCMA	Interim Defense Acquisition Guidebook	Defense Contract Management Agency
DCS	AT Implementation Guidelines, USD, May 00	Direct Commercial Sales
DCS		Direct Commercial Sales
DDR&E		Director of Defense Research and Engineering
DEW	Interim Defense Acquisition Guidebook	Directed Energy Weapon
DFARS	Interim Defense Acquisition Guidebook	Defense Federal Acquisition Regulation Supplement
DIA	Interim Defense Acquisition Guidebook	Defense Intelligence Agency
DIA	CJCSI 3170.01D, Mar 04	Defense Intelligence Agency
DIAC		Defense Intelligence Analysis Center
DIAP		Defense-Wide Infrastructure Assurance Program
DIRNSA		Director, National Security Agency
DISA	Interim Defense Acquisition Guidebook	Defense Information Systems Agency
DITSCAP		DoD Information Technology Security Certification & Accreditation Process
DJSM	CJCSI 3170.01D, Mar 04	Director, Joint Staff memorandum
DLA	Interim Defense Acquisition Guidebook	Defense Logistics Agency
DoD	AT Implementation Guidelines, USD, May 00	Department of Defense; the Department
DoD	Interim Defense Acquisition Guidebook	Department of Defense
DoD CIO	Interim Defense Acquisition Guidebook	Department of Defense Chief Information Officer
DoDD	AFPD 63-1, Jul 03	Department of Defense Directive
DoDI	AFPD 63-1, Jul 03	Department of Defense Instruction
DOT&E	CJCSI 3170.01D, Mar 04	Director of Operational Test and Evaluation.

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
DOT&E	Interim Defense Acquisition Guidebook	Director, Operational Test and Evaluation
DOTMLPF	CJCSI 3170.01D, Mar 04	doctrine, organization, training, materiel, leadership and education, personnel and facilities
DSS		Defense Security Service
DT	Interim Defense Acquisition Guidebook	Developmental Testing
DT&E	Interim Defense Acquisition Guidebook	Developmental Test and Evaluation
DUSD(IA)	Interim Defense Acquisition Guidebook	Deputy Under Secretary of Defense (Industrial Affairs)
DUSD(S&T)	Interim Defense Acquisition Guidebook	Deputy Under Secretary of Defense (Science and Technology)
E.O.	Interim Defense Acquisition Guidebook	Executive Order
E3	Interim Defense Acquisition Guidebook	Electromagnetic Environmental Effects
EA	AFPD 63-1, Jul 03	Evolutionary Acquisition
EA	Interim Defense Acquisition Guidebook	Economic Analysis
EAP		Employee Assistance Program
EC		Electronic Commerce
EDI		Electronic Data Interchange
EEFI	DoD 5200.1-M, Mar 94	Essential Elements of Friendly Information
EPITS	DoD 5200.1-M, Mar 94	Essential Program Information, Technologies, and/or Systems
ESOH	Interim Defense Acquisition Guidebook	Environment, Safety, and Occupational Health
EVMS	Interim Defense Acquisition Guidebook	Earned Value Management System
EW	Interim Defense Acquisition Guidebook	Electronic Warfare

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
FAA	CJCSI 3170.01D, Mar 04	functional area analysis
FACA	Interim Defense Acquisition Guidebook	Federal Advisory Committee Act
FAR	Interim Defense Acquisition Guidebook	Federal Acquisition Regulation
FCB	CJCSI 3170.01D, Mar 04	Functional Capabilities Board
FCT	Interim Defense Acquisition Guidebook	Foreign Comparative Testing
FFP	Interim Defense Acquisition Guidebook	Firm Fixed-Price
FFRDC		Federally Funded Research and Development Center
FMS	AT Implementation Guidelines, USD, May 00	Foreign Military Sales Program
FMS		Foreign Military Sales Program
FNA	CJCSI 3170.01D, Mar 04	functional needs analysis
FoS	CJCSI 3170.01D, Mar 04	family of systems
FOT&E	Interim Defense Acquisition Guidebook	Follow-On Operational Test and Evaluation
FOUO		For Official Use Only
FSA	CJCSI 3170.01D, Mar 04	functional solution analysis
FTE		Full-Time Equivalent
FYDP	Interim Defense Acquisition Guidebook	Future Years Defense Program
GCCS	CJCSI 3170.01D, Mar 04	Global Command and Control System
GIG	Interim Defense Acquisition Guidebook	Global Information Grid
GIG	CJCSI 3170.01D, Mar 04	Global Information Grid
GOCO	AFPD 63-17, Nov 01	Government Owned Contractor Operated
GOTS		Government Off The Shelf
GPPC	Interim Defense Acquisition Guidebook	Government Property in the Possession of Contractors
GPRA		Government Performance and Results Act

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
HEMP	Interim Defense Acquisition Guidebook	High Altitude Electromagnetic Pulse
HFE	Interim Defense Acquisition Guidebook	Human Factors Engineering
HSI	Interim Defense Acquisition Guidebook	Human Systems Integration
HUMINT	DoD 5200.1-M, Mar 94	human intelligence
I&W		indications and warning
IA		information assurance
ICD	CJCSI 3170.01D, Mar 04	Initial Capabilities Document
IDE	Interim Defense Acquisition Guidebook	Integrated Digital Environment
IDS		Intrusion Detection System
IER	Interim Defense Acquisition Guidebook	Information Exchange Requirement
IIPT	Interim Defense Acquisition Guidebook	Integrating Integrated Product Team
INFOSEC		information security
IOC	Interim Defense Acquisition Guidebook	Initial Operational Capability
IOT&E	CJCSI 3170.01D, Mar 04	initial operational test and evaluation
IOT&E	Interim Defense Acquisition Guidebook	Initial Operational Test and Evaluation
IPL	CJCSI 3170.01D, Mar 04	integrated priority list
IPPD	Interim Defense Acquisition Guidebook	Integrated Product and Process Development
IPT	Interim Defense Acquisition Guidebook	Integrated Product Team
IS		Information System
ISM	DoD 5200.1-M, Mar 94	Industrial Security Manual
ISP		Internet Service Provider
ISP	CJCSI 3170.01D, Mar 04	Information Support Plan

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
ISSM		Information System Security Manager
ISSO		Information System Security Officer
IT	Interim Defense Acquisition Guidebook	Information Technology
IT		Information Technology
IT	CJCSI 3170.01D, Mar 04	information technology
IT OIPT	Interim Defense Acquisition Guidebook	Information Technology Overarching Integrated Product Team
ITAB	CJCSI 3170.01D, Mar 04	Information Technology Acquisition Board
ITAR		International Traffic in Arms Regulation
JC2	CJCSI 3170.01D, Mar 04	Joint Command and Control
JCB	CJCSI 3170.01D, Mar 04	Joint Capabilities Board
JCIDS	CJCSI 3170.01D, Mar 04	Joint Capabilities Integration and Development System
JCPAT	Interim Defense Acquisition Guidebook	Joint C4ISP Assessment Tool
JFC	CJCSI 3170.01D, Mar 04	Joint Functional Concept
JIC	CJCSI 3170.01D, Mar 04	Joint Integrating Concept
JITC	Interim Defense Acquisition Guidebook	Joint Interoperability Test Command
JOC	CJCSI 3170.01D, Mar 04	Joint Operating Concept
JOpsC	CJCSI 3170.01D, Mar 04	Joint Operations Concepts
JPD	CJCSI 3170.01D, Mar 04	Joint Potential Designator
JPG	CJCSI 3170.01D, Mar 04	Joint Programming Guidance
JROC	CJCSI 3170.01D, Mar 04	Joint Requirements Oversight Council
JROC	Interim Defense Acquisition Guidebook	Joint Requirements Oversight Council
JROCM	CJCSI 3170.01D, Mar 04	JROC memorandum
JTA	Interim Defense Acquisition Guidebook	Joint Technical Architecture
JWSTP	CJCSI 3170.01D, Mar 04	Joint Warfighting Science and Technology Plan
KDP	CJCSI 3170.01D, Mar 04	Key Decision Point
KM/DS	CJCSI 3170.01D, Mar 04	Knowledge Management/Decision Support

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
KPP	Interim Defense Acquisition Guidebook	Key Performance Parameter
KPP	CJCSI 3170.01D, Mar 04	key performance parameter
LAC		Local Agency Check
LCCE	Interim Defense Acquisition Guidebook	Life-Cycle Cost Estimate
LFT&E	Interim Defense Acquisition Guidebook	Live Fire Test and Evaluation
LOA	AT Implementation Guidelines, USD, May 00	Letter of Offer and Acceptance
LOA		Letter of Offer and Acceptance
LRIP	Interim Defense Acquisition Guidebook	Low-Rate Initial Production
M&S	Interim Defense Acquisition Guidebook	Modeling and Simulation
MAIS	Interim Defense Acquisition Guidebook	Major Automated Information System
MAJCOM	AFPD 63-1, Jul 03	Major Command
MCEB	Interim Defense Acquisition Guidebook	Military Communications-Electronics Board
MDA	AT Implementation Guidelines, USD, May 00	Milestone Decision Authority
MDA	CJCSI 3170.01D, Mar 04	Milestone Decision Authority
MDA	Interim Defense Acquisition Guidebook	Milestone Decision Authority
MDAP	Interim Defense Acquisition Guidebook	Major Defense Acquisition Program
MDCI	DoD 5200.1-M, Mar 94	Multi-Discipline Counterintelligence
MilDep	Interim Defense Acquisition Guidebook	Military Department
MNS	CJCSI 3170.01D, Mar 04	Mission Need Statement

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
MNS	Interim Defense Acquisition Guidebook	Mission Needs Statement
MOA	AT Implementation Guidelines, USD, May 00	Memorandum of Agreement
MOA	Interim Defense Acquisition Guidebook	Memorandum of Agreement
MOE	CJCSI 3170.01D, Mar 04	measures of effectiveness
MOE	Interim Defense Acquisition Guidebook	Measure of Effectiveness
MOP	Interim Defense Acquisition Guidebook	Measure of Performance
MOU	AT Implementation Guidelines, USD, May 00	Memorandum of Understanding
MOU	Interim Defense Acquisition Guidebook	Memorandum of Understanding
MRB	CJCSI 3170.01D, Mar 04	Mission Requirements Board
NAC		National Agency Check
NACI		National Agency Check plus Written Inquiries
NACLC		National Agency Check with Local Agency Check
NATO	Interim Defense Acquisition Guidebook	North Atlantic Treaty Organization
NBC	Interim Defense Acquisition Guidebook	Nuclear, Biological, and Chemical
NDP	DoD 5200.1-M, Mar 94	National Disclosure Policy
NEO	Interim Defense Acquisition Guidebook	Noncombatant Evacuation Operation
NEPA	Interim Defense Acquisition Guidebook	National Environmental Policy Act
NFIP	CJCSI 3170.01D, Mar 04	National Foreign Intelligence Program
NIAP		National Information Assurance Partnership (NIAP)
NIC	Interim Defense Acquisition Guidebook	Notice of Intent to Conclude

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
NIMA	Interim Defense Acquisition Guidebook	National Imagery and Mapping Agency
NIN	Interim Defense Acquisition Guidebook	Notice of Intent to Negotiate
NISP	DoD 5200.1-M, Mar 94	National Industrial Security Program
NOCONTRACT	DoD 5200.1-M, Mar 94	Not Releasable to Contractors and/or Consultants
NR-KPP	CJCSI 3170.01D, Mar 04	Net-Ready Key Performance Parameter
NSA		National Security Agency
NSS	CJCSI 3170.01D, Mar 04	National Security Systems
NSS	Interim Defense Acquisition Guidebook	National Security Systems
NSTISSC		National Security Telecommunications and Information Systems Security Committee
OA	Interim Defense Acquisition Guidebook	Operational Assessment
OASD	CJCSI 3170.01D, Mar 04	Office of the Assistant Secretary of Defense
OASD(C3I)	DoD 5200.1-M, Mar 94	Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
OCR		Office of Collateral Responsibility
OGA		other government agencies
OGC		Office of General Counsel, OSD
OIPT	AT Implementation Guidelines, USD, May 00	Overarching Integrated Product Team
OIPT	Interim Defense Acquisition Guidebook	Overarching Integrated Product Team
OMB		Office of Management and Budget
OPFAC	Interim Defense Acquisition Guidebook	Operational Facility
OPM		Office of Personnel Management
OPR		Office of Primary Responsibility
OPSEC		Operations Security

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
OPSIT	Interim Defense Acquisition Guidebook	Operational Situation
ORCON	DoD 5200.1-M, Mar 94	Dissemination and Extraction of Information Controlled by Originator
ORD	CJCSI 3170.01D, Mar 04	Operational Requirements Document
ORD	Interim Defense Acquisition Guidebook	Operational Requirements Document
OSD	CJCSI 3170.01D, Mar 04	Office of the Secretary of Defense
OSD	Interim Defense Acquisition Guidebook	Office of the Secretary of Defense
OT	Interim Defense Acquisition Guidebook	Operational Testing
OT&E	Interim Defense Acquisition Guidebook	Operational Test and Evaluation
OTA	Interim Defense Acquisition Guidebook	Operational Test Agency
OTRR	Interim Defense Acquisition Guidebook	Operational Test Readiness Review
OUSD		Office of the Undersecretary of Defense
OUSD	CJCSI 3170.01D, Mar 04	Office of the Under Secretary of Defense
OUSD(A&T)	DoD 5200.1-M, Mar 94	Office of the Under Secretary of Defense for Acquisition and Technology
OUSD(AT&L)	AT Implementation Guidelines, USD, May 00	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
OUSD(AT&L)		Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
OUSD(P&R)	Interim Defense Acquisition Guidebook	Office of the Under Secretary of Defense (Personnel & Readiness)
P3I	AT Implementation Guidelines, USD, May 00	Pre-Planned Product Improvement
P3I		Pre-Planned Product Improvement
PA		Project Arrangement

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
PA	AT Implementation Guidelines, USD, May 00	Project Arrangement
PA&E	CJCSI 3170.01D, Mar 04	program analysis and evaluation
PA&E	Interim Defense Acquisition Guidebook	Program Analysis and Evaluation
PAUC	Interim Defense Acquisition Guidebook	Program Acquisition Unit Cost
PBBE	Interim Defense Acquisition Guidebook	Performance-Based Business Environment
PBL	Interim Defense Acquisition Guidebook	Performance-Based Logistics
PEO	AT Implementation Guidelines, USD, May 00	Program Executive Officer
PEO	Interim Defense Acquisition Guidebook	Program Executive Officer
PESHE	Interim Defense Acquisition Guidebook	Programmatic Environment, Safety, and Occupational Health Evaluation
PKI		Public Key Infrastructure
PM	AT Implementation Guidelines, USD, May 00	Program Manager
PM	Interim Defense Acquisition Guidebook	Program Manager
PMD	AFPD 63-17, Nov 01	Program Management Directive
PNO	Interim Defense Acquisition Guidebook	Program Number
POC	Interim Defense Acquisition Guidebook	Point of Contact
POM	Interim Defense Acquisition Guidebook	Program Objective Memorandum
PPBE	CJCSI 3170.01D, Mar 04	Planning, Programming, Budgeting, and Execution
PPP	AT Implementation Guidelines, USD, May 00	Program Protection Plan

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
PR		Periodic Reinvestigation
PROPIN	DoD 5200.1-M, Mar 94	Proprietary Information Involved
PSA	Interim Defense Acquisition Guidebook	Principal Staff Assistant
PSO		Program Security Officer
R&D		Research & Development
RAD	Interim Defense Acquisition Guidebook	Request for Authority to Develop and Negotiate
RAM	Interim Defense Acquisition Guidebook	Reliability, Availability, and Maintainability
RCS	Interim Defense Acquisition Guidebook	Report Control Symbol
RDT&E	Interim Defense Acquisition Guidebook	Research, Development, Test and Evaluation
RFA	Interim Defense Acquisition Guidebook	Request for Final Approval
RFP	Interim Defense Acquisition Guidebook	Request for Proposal
ROI	Interim Defense Acquisition Guidebook	Return on Investment
S&T		Science and Technology, or Science and Technical
S&TS		Strategic and Tactical Systems
S&TS	AT Implementation Guidelines, USD, May 00	Strategic and Tactical Systems
SAE	Interim Defense Acquisition Guidebook	Service Acquisition Executive
SAMP	Interim Defense Acquisition Guidebook	System Acquisition Master Plan
SAP	AT Implementation Guidelines, USD, May 00	Special Access Program
SAP		Special Access Program

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
SAR	Interim Defense Acquisition Guidebook	Special Access Required
SBA	Interim Defense Acquisition Guidebook	Simulation-Based Acquisition
SBIR	Interim Defense Acquisition Guidebook	Small Business Innovation Research
SBU		Sensitive But Unclassified
SCG		Security Classification Guide
SCI	AFPD 63-17, Nov 01	Sensitive Comparmented Information
SCO		Senior Civilian Official
SDD	CJCSI 3170.01D, Mar 04	System Development and Demonstration
SECAF	AFPD 63-1, Jul 03	Secretray of the Air Force
SEI	Interim Defense Acquisition Guidebook	Software Engineering Institute
SEMP	DoD 5200.1-M, Mar 94	System Engineering Management Plan
SF-85PS		Standard Form - 85 Supplemental Questionnaire for Selected Positions
SM	AFPD 63-1, Jul 03	Single Manager
SoS s	CJCSI 3170.01D, Mar 04	ystem of systems
SPD	AFPD 63-1, Jul 03	System Program Director
SPG	CJCSI 3170.01D, Mar 04	Strategic Planning Guidance
SPO	AFPD 63-17, Nov 01	System Program Office
SRC		Security Research Center, OSD/P&R
SSAA	Interim Defense Acquisition Guidebook	System Security Authorization Agreement
SSBI		Single Scope Background Investigation
SSE	DoD 5200.1-M, Mar 94	System Security Engineering
SSEM	DoD 5200.1-M, Mar 94	System Security Engineering Manager
SSMP	DoD 5200.1-M, Mar 94	System Security Management Plan
SSOI	Interim Defense Acquisition Guidebook	Summary Statement of Intent
STAR	DoD 5200.1-M, Mar 94	System Threat Assessment Report

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
STT	Interim Defense Acquisition Guidebook	Statement-to-Task
STU	DoD 5200.1-M, Mar 94	Secure Telephone Unit
SUPSHIP	Interim Defense Acquisition Guidebook	Supervisor of Shipbuilding, Conversion, and Repair
T&E	Interim Defense Acquisition Guidebook	Test and Evaluation
TA/CP	DoD 5200.1-M, Mar 94	Technology Assessment/Control Plan
TDD	AFPD 63-17, Nov 01	Technical Directorate Director
TEMP	Interim Defense Acquisition Guidebook	Test and Evaluation Master Plan
TOC	Interim Defense Acquisition Guidebook	Total Ownership Cost
TPP	AFPD 63-17, Nov 01	Technology Protection Plan
TRL	Interim Defense Acquisition Guidebook	Technology Readiness Level
U.S.C.	Interim Defense Acquisition Guidebook	United States Code
UCR	Interim Defense Acquisition Guidebook	Unit Cost Report
UJTL	CJCSI 3170.01D, Mar 04	Universal Joint Task List
USD(A&T)	DoD 5200.1-M, Mar 94	Under Secretary of Defense for Acquisition and Technology
USD(AT&L)	Interim Defense Acquisition Guidebook	Under Secretary of Defense (Acquisition, Technology, and Logistics)
USD(AT&L)	CJCSI 3170.01D, Mar 04	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	CJCSI 3170.01D, Mar 04	Under Secretary of Defense for Intelligence
USD(P)	DoD 5200.1-M, Mar 94	Under Secretary of Defense for Policy
USecAF	CJCSI 3170.01D, Mar 04	Under Secretary of the Air Force
USJFCOM	CJCSI 3170.01D, Mar 04	United States Joint Forces Command
USJFCOM	Interim Defense Acquisition Guidebook	United States Joint Forces Command

ACRONYMS

Includes definitions from DoD 5200.1-M, DoDD 5025.1-M, DoDD 4630.5, DoDD 8500.1, DoDD 5000.1, DoDD 5200.1, DoDD 5200.39, DoDD 5205.2, AFPD 63-1, AFPD 63-17, AT Implementation Guidelines, and the Interim Defense Acquisition Guidebook.

Acronym	Reference	Definition
USSOCOM	CJCSI 3170.01D, Mar 04	United States Special Operations Command
V&V	AT Implementation Guidelines, USD, May 00	Verification and Validation
V&V		Verification and Validation
VVA	Interim Defense Acquisition Guidebook	Verification, Validation, and Accreditation
WBS	Interim Defense Acquisition Guidebook	Work Breakdown Structure
WHS	Interim Defense Acquisition Guidebook	Washington Headquarters Services
WIPT	Interim Defense Acquisition Guidebook	Working-Level Integrated Product Team
WRM	DoD 5200.1-M, Mar 94	Wartime Reserve Mode

Technology Readiness Level	Description
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.
7. System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.